DISEÑO DE UN MARCO METODOLÓGICO PARA LA IMPLEMENTACIÓN DE UNA ESTRATEGIA DE RESPALDO DE INFORMACIÓN

JHON LENNON GOMEZ IGUARAN

ANIBAL RAMÓN MAURY PÉREZ

UNIVERSIDAD DE LA COSTA CUC

DEPARTAMENTO DE POSTGRADOS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BARRANQUILLA

2013

DISEÑO DE UN MARCO METODOLÓGICO PARA LA IMPLEMENTACIÓN DE UNA ESTRATEGIA DE RESPALDO DE INFORMACIÓN

JHON LENNON GOMEZ IGUARAN

ANIBAL RAMÓN MAURY PÉREZ

Proyecto presentado como requisito para optar el título de Especialista en Auditoría de Sistemas de Información.

Victor Montaño
Asesor

UNIVERSIDAD DE LA COSTA CUC

DEPARTAMENTO DE POSTGRADOS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN

BARRANQUILLA

2013

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Jurado

_____

Jurado

Barranquilla, Enero 14 de 2014

AGRADECIMIENTOS

Principalmente le damos gracias principalmente a Dios quien ha iluminado nuestro camino día a día con todas las bendiciones, que han hecho que mi vida llegue hasta este momento tan importante y que se proyecte hacia un futuro exitoso.

Gracias a nuestras familias quienes estuvieron en todos los momentos de gloria, de tristeza, de felicidad, principalmente a nuestras madres quienes fueron un apoyo incondicional en toda nuestra carrera y han me ha enseñado con su sabiduría a ser una persona trabajadora, responsable y honesta.

Gracias a la Universidad De La Costa CUC por brindarnos el apoyo y las herramientas necesarias para lograr ser unos profesionales distinguidos y sobresalientes, apoyando todos los procesos académicos de la formación como persona y como profesional.

ANIBAL MAURY PEREZ

JHON GOMEZ IGUARAN

TABLA DE CONTENIDO

Pág.

TABLA DE FIGURAS

1. INTRODUCCION

La información se ha convertido en un activo estratégico de las empresas, un activo que tiene un valor en ocasiones poco calculable hasta que se pierde y altera la trayectoria del negocio. Esta pérdida puede ser ocasionada por diferentes factores como condiciones atmosféricas extremas, actividades políticas hostiles, pérdida de los sistemas y datos informáticos, pérdida de poder, pérdida de una persona esencial, incendio, inundación o una explosión.

Según datos del Emergency Management Forum [1], el 43% de las empresas estadounidenses que afrontan un desastre sin contar con un Plan de Continuidad de Negocio nunca vuelven a la actividad, el 51% sobrevive pero tarda un promedio de dos años para reinsertarse en el mercado y sólo el 6% mantiene su negocio a largo plazo.

Actualmente, las autoridades reguladoras están insistiendo en que se adopten medidas que protejan a las organizaciones de sucesos imprevistos y a medida que los negocios evolucionan, también lo hace la dependencia a las infraestructuras de soporte. Como ejemplo sencillo, la pérdida del correo electrónico hace diez años podría haber sido una incomodidad. Hoy en día, el correo electrónico se ha convertido en un medio de comunicación fundamental para la mayoría de las organizaciones, independientemente de su tamaño, y ha sido una herramienta decisiva en el desarrollo de los mercados de alcance global.

1.1. FORMULACION DEL PROBLEMA

Un incidente no tiene que ser un dramático ataque terrorista para tener un impacto enorme en una empresa. La idea fundamental es que las empresas necesitan implementar planes que les permitan manejar incidentes, ya sean grandes ataques terroristas o pequeños problemas informáticos y, por tanto, evitar grandes interrupciones del negocio. Por esta razón, se han desarrollado directivas y estándares para la Gestión de la Continuidad del Negocio [2], que es el nombre que se da a las distintas disciplinas que tienen como objetivo promover políticas, prácticas y procesos que estén al servicio de las medidas de protección que hoy en día existen en los mercados financieros y que deben ser adoptadas por las organizaciones. Algunos de estos estándares son **British Standard - 25999** [3] para la Gestión de la Continuidad del Negocio, el proceso de "Gestión de la continuidad de los servicios IT" en la etapa de "Diseño del servicio" de **ITIL** [4] o el proceso "DS4 - Asegurar la continuidad del servicio" del dominio "Entrega y soporte" del estándar **COBIT** [5].

Para las grandes organizaciones, la gestión de la continuidad del negocio se lleva a cabo durante todo el tiempo, por una persona o un pequeño equipo (de acuerdo al tamaño del negocio). Pero para la gran mayoría de las empresas, esta función será probablemente la responsabilidad de una persona que haga este trabajo además de sus funciones diarias, o algunas ni siquiera tienen contemplado un plan de continuidad, debido a la falta de formación y de información sencilla, detallada y que ilustre las fases, tareas y actividades para confeccionar un Plan de continuidad ágilmente.

2. JUSTIFICACION

En la actualidad, la creciente competitividad entre las organizaciones, las demandas de los clientes cada vez más exigentes o los requerimientos normativos rigurosos son factores que obligan a las empresas a adoptar nuevas estrategias a fin de garantizar el éxito y demostrar la resistencia de las operaciones de negocio ante cualquier eventualidad grave. Sin embargo, acorde con la experiencia de los autores de este escrito y la literatura existente en la materia, el nivel de implantación de planes de continuidad de negocio en las pequeñas y medianas empresas es notablemente inferior si se compara con las grandes empresas quienes disponen de los recursos técnicos, económicos y humanos necesarios para convertir esta necesidad en una realidad.

Si bien existen multitud de manuales, estándares y recomendaciones que tratan de guiar a las organizaciones a adoptar estrategias de continuidad de negocio, la mayoría de ellas son teóricas, expresadas con un lenguaje formal, y no tienen en cuenta la situación, problemática, necesidades reales o niveles de conocimiento de las organizaciones.

Este proyecto de carácter académico, busca disminuir estos niveles de desorientación, a través de un marco de metodológico de actuación para aquellas organizaciones (sin importar el sector, actividad, ubicación geográfica, ni tamaño) que deseen entender y abordar los principios y las prácticas de continuidad de negocio desde el momento en que se reconoce la necesidad de desarrollar una estrategia de continuidad, hasta su mantenimiento y actualización constante.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Diseñar un marco metodológico para la implementación de una estrategia de respaldo de información en una compañía, soportado en estándares de Gestión de la Continuidad del Negocio.

3.2. OBJETIVOS ESPECIFICOS

Explorar e interpretar el proceso Gestión de la Continuidad de los Servicios de TI de ITIL y el proceso “DS11 - Administración de Datos” del dominio “Entrega y soporte” de COBIT. A partir de dicha exploración:

- Diseñar un Marco Metodológico para la implementación de una estrategia de respaldo información adaptable a cualquier empresa.
- Desarrollar una guía de implantación de dicho marco, donde se muestren cada una de las fases que componen la estrategia de respaldo.
- Describir las actividades a desarrollar en cada una de las fases de la implementación de la estrategia de respaldo.

4. MARCO TEORICO

4.1. DEFINICIONES

AMENAZA: eventos que, aprovechando una vulnerabilidad, pueden desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos. Dentro de eventos se consideran tanto acciones, como interrupciones o falta de acción.

DESASTRE: problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un periodo de tiempo. Este tiempo de paralización de los procesos es superior a lo que la organización puede soportar sin sufrir perjuicios considerables para el negocio.

GOBIERNO DE TI: Consiste en un completo marco de estructuras, procesos y mecanismos relacionales. Las estructuras implican la existencia de funciones de responsabilidad, como los ejecutivos y responsables de las cuentas de TI, así como diversos comités de TI. Los procesos se refieren a la monitorización y a la toma de decisiones estratégicas de TI. Los mecanismos relacionales incluyen las alianzas y la participación de la empresa/organización de TI, el dialogo en la estrategia y el aprendizaje compartido. [6]

GESTION DE LA CONTINUIDAD: es un proceso integral que identifica los impactos potenciales que amenazan una organización y proporciona un marco para la construcción de la resiliencia y la capacidad para dar una respuesta eficaz que salvaguarde los intereses de sus principales partes interesadas, la reputación, la marca y el valor de la creación de actividades.

IMPACTO: consecuencia evaluada de una interrupción.

INCIDENTE: cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción o una reducción de la calidad de ese servicio.

INTERDEPENDENCIAS: relaciones establecidas entre el conjunto de equipamiento, personas, tareas, departamentos, mecanismos de comunicación y proveedores externos que constituye una actividad de negocio.

INTERRUPCIÓN: suspensión de las operaciones normales del negocio durante un período de tiempo.

PLAN DE CONTINUIDAD DE NEGOCIO (PCN) o BUSINESS CONTINUITY PLAN (BCP por sus siglas en inglés) es un conjunto de directrices, criterios, normas de actuación y herramientas organizativas que, ante la ocurrencia de una contingencia que provocase la interrupción de alguna o todas las áreas de negocio de una organización, permiten la recuperación de la operatividad de las mismas en el menor tiempo posible, de modo que las pérdidas económicas ocasionadas sean mínimas.

RESILIENCIA: término de origen inglés (resilient) referido a la capacidad de elasticidad y resistencia de una empresa para hacer frente a los impactos.

RIESGO: probabilidad de que una amenaza aproveche y explote una debilidad asociada a un proceso/activo/recurso provocando daño sobre el mismo.

TELETRABAJO: desempeño de un trabajo de manera regular en un lugar diferente del centro de trabajo habitual, generalmente empleando medios informáticos.

VULNERABILIDAD: debilidad o falta de control asociada a un proceso o recurso que puede ser explotada provocando un daño sobre dicho proceso.

4.2. GENERALIDADES

La Gestión de Continuidad de Negocio es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización y ofrece un marco para proporcionar robustez y disponer de una respuesta efectiva que salvaguarde los intereses de los principales proveedores, clientes y demás partes interesadas, la reputación, la marca y las actividades creadoras de valor.

La GCN tiene que ser asimilada y totalmente integrada en la organización como uno más entre sus procesos de gestión.

La GCN aspira a mejorar la capacidad de recuperación de una organización. Al identificar por adelantado los posibles impactos de una amplia gama de incidencias que trastornarían de forma súbita el éxito de la organización, establece prioridades para los esfuerzos de los especialistas en implantar robustez en sus respectivas áreas de especialización, como seguridad, instalaciones y tecnologías de la información.

Si bien se interesa por todo tipo de mecanismos de fortaleza o robustez, la GCN se centra particularmente en desarrollar una capacidad de recuperación que sea conjunta para toda la organización y le permita sobrevivir a la pérdida total o parcial de su capacidad operativa. También debería enfocarse en soportar pérdidas significativas de recursos, como personal o maquinaria.

Debido a que la capacidad de resistencia de la GCN de una organización depende de su equipo de gestión y su personal, además de su tecnología y la diversificación geográfica, se debe desarrollar esta capacidad de recuperación a

todos los niveles de la organización, desde la alta dirección hasta el taller, y en todos los demás integrantes de la cadena de valor.

El factor determinante de esta robustez en toda la organización se sustenta en la responsabilidad de la alta dirección de proteger los intereses a largo plazo del personal, clientes y todos aquellos que dependen de algún modo de la organización. Si bien se pueden calcular las pérdidas financieras ocasionadas por una interrupción, generalmente el mayor daño suele reflejarse en una pérdida de imagen o de confianza fruto de un incidente mal gestionado. Del mismo modo, un incidente bien gestionado puede mejorar la imagen de la organización y su equipo de gestión.

La base de la gestión de la continuidad son las políticas, guías, estándar y procedimientos implementados por una organización. Todo el diseño, implementación, soporte y mantenimiento de los sistemas debe estar fundamentado en la obtención de un buen plan de continuidad del negocio, recuperación de desastres y en algunos casos, soporte al sistema. En ocasiones la gestión de la continuidad se confunde con la gestión de la recuperación tras un desastre, pero son conceptos diferentes. La recuperación de desastres es una pequeña parte de la gestión de la continuidad.

Los objetivos principales de la Gestión de la Continuidad se resumen en: garantizar la pronta recuperación de los servicios (críticos) tras un desastre, establecer políticas y procedimientos que eviten, en la medida de lo posible, las consecuencias de un desastre o causa de fuerza mayor.

Los principales beneficios de una correcta Gestión de la Continuidad se resumen en: se gestionan adecuadamente los riesgos, se reduce el periodo de interrupción del servicio por causas de fuerza mayor, se mejora la confianza en la calidad del servicio entre clientes y usuarios.

Las principales dificultades a la hora de implementar la Gestión de la Continuidad se resumen en: puede haber resistencia a realizar inversiones cuya rentabilidad no es inmediata, no se presupuestan correctamente los costos asociados, no se asignan los recursos suficientes, no existe el compromiso suficiente con el proceso dentro de la organización y las tareas y actividades correspondientes se demoran perpetuamente para hacer frente a "actividades más urgentes", no se realiza un correcto análisis de riesgos y se obvian amenazas y vulnerabilidades reales, el personal no está familiarizado con las acciones y procedimientos a tomar en caso de interrupción grave de los servicios.

La Gestión de la Continuidad está destinada al fracaso sino se destina una cantidad de recursos suficientes, tanto en el plano humano como de equipos. Su dimensión depende de su alcance y sería absurdo instaurar una política demasiado ambiciosa que no cuente con los recursos correspondientes.

En la actualidad casi todas las empresas, grandes y pequeñas, dependen en mayor o menor medida de los servicios informáticos, por lo que cabe esperar que una interrupción de los servicios TI afecte a prácticamente todos los aspectos del negocio. Sin embargo, es evidente que hay servicios TI estratégicos de cuya continuidad puede depender la supervivencia del negocio y otros que simplemente aumentan la productividad de la fuerza comercial y de trabajo.

El objetivo de la Gestión de la Continuidad de TI es apoyar los procesos empresariales, asegurando que las instalaciones técnicas y de servicio de TI (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, apoyo técnico y mesa de servicios) se puedan reanudar, según los plazos de tiempo acordados. Los servicios TI no son sino una parte, aunque a menudo muy importante, del negocio.

Es importante diferenciar entre desastres como incendios, inundaciones, etc., y desastres "puramente informáticos", tales como los producidos por ataques distribuidos de denegación de servicio o virus informáticos. Aunque es responsabilidad de la ITSCM prever los riesgos asociados en ambos casos y restaurar el servicio TI con prontitud, es evidente que recae sobre la ITSCM una responsabilidad especial en el último caso pues: sólo afectan directamente a los servicios TI pero paralizan a toda la organización, son más previsibles y más habituales, la percepción del cliente es diferente: los desastres naturales son más asumibles y no se asocian a actitudes negligentes, aunque esto no sea siempre cierto.

4.3. ITIL

Information Technology Infrastructure Library (ITIL) es un marco de trabajo que define los mejores prácticas y enfoques de la gestión de Tecnologías de la Información (TI). Detalla la forma en que la Gestión de Servicios TI (ITSM) puede ser implementada en una empresa para mejorar la calidad de los servicios de TI por las personas que utilizan software, servicios y metodologías de forma colectiva. [10] Su objetivo es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible.

Sus orígenes se remontan a la década de los 80 cuando el gobierno británico, preocupado por la calidad de los servicios TI de los que dependía la administración, solicito a una de sus agencias, la CCTA acrónimo de Central Computer and Telecommunications Agency, para que desarrollara un estándar para la provisión eficiente de servicios TI. En la actualidad es la OGC (Office of Government Commerce) el organismo encargado de velar por este estándar y la responsable de la última versión de ITIL (v3) que data del año 2007.

ITIL implementa diferentes procesos de Gestión de Servicios de TI, tales como la gestión del ciclo de vida y solicitud de gestión para mejorar la calidad de los servicios de TI. El componente básico contiene cinco estrategias de gestión del marco de ITIL, que representan el ciclo de vida de servicios de TI. Las diferentes estrategias de manejo son:

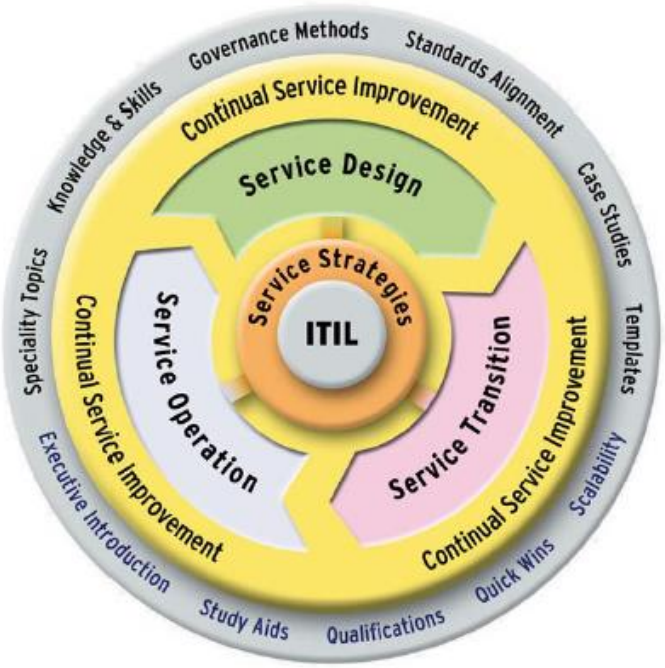


Figura 1. Ciclo de Vida de la Gestión de Servicio de TI – ITIL

- **Estrategia del servicio**. Ayuda a la compañía a planificar la implementación de estrategias de gestión de servicios de TI. Permite definir nuevos servicios de TI y ayudar a asegurar que la los servicios de TI actualmente establecidos satisfacen las necesidades de la empresa.

- **Diseño del Servicio.** Ayuda a crear políticas, arquitecturas y diseños para los servicios de TI para satisfacer las necesidades actuales y futuras de una empresa.

- **Transición del Servicio.** Ayuda a gestionar y controlar los cambios en los servicios de TI que se implementan en el entorno de trabajo de una empresa y asegurar la continuidad de los servicios de TI cuando se produzcan cambios.

- **Operación del Servicio.** Asegurar que los servicios de TI se ofrezcan efectiva y eficientemente. Esto incluye cumplir con los requerimientos de los usuarios,

resolver fallos en el servicio, arreglar problemas y llevar a cabo operaciones rutinarias del día a día.

- **Mejora continua del servicio.** Ayuda a lograr una mejor calidad de servicios de TI en una empresa, identificando y evaluando iniciativas, medidas correctivas y cumplimiento de metas que mejoren la efectividad y eficiencia de procesos y servicios de TI.

En la etapa de Diseño del Servicio se define el proceso **Gestión de la Continuidad de los Servicios de TI (ITSCM),** en el cual se establecen planes de contingencia que aseguren la continuidad del servicio en un tiempo predeterminado con el menor impacto posible en los servicios de carácter crítico. El objetivo de ITSCM es apoyar la continuidad, la gestión de procesos empresariales, asegurando las instalaciones que requiere servicios técnicos (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, apoyo técnico y mesa de servicios), reduciendo el riesgo de eventos desastrosos hasta niveles aceptables y planificando la recuperación en caso de que ocurran. ITSCM se centra en los eventos que la empresa considera lo suficientemente importantes como para ser considerado un desastre. Los eventos menos importantes se tratarán como parte del proceso de Gestión de Incidencias.

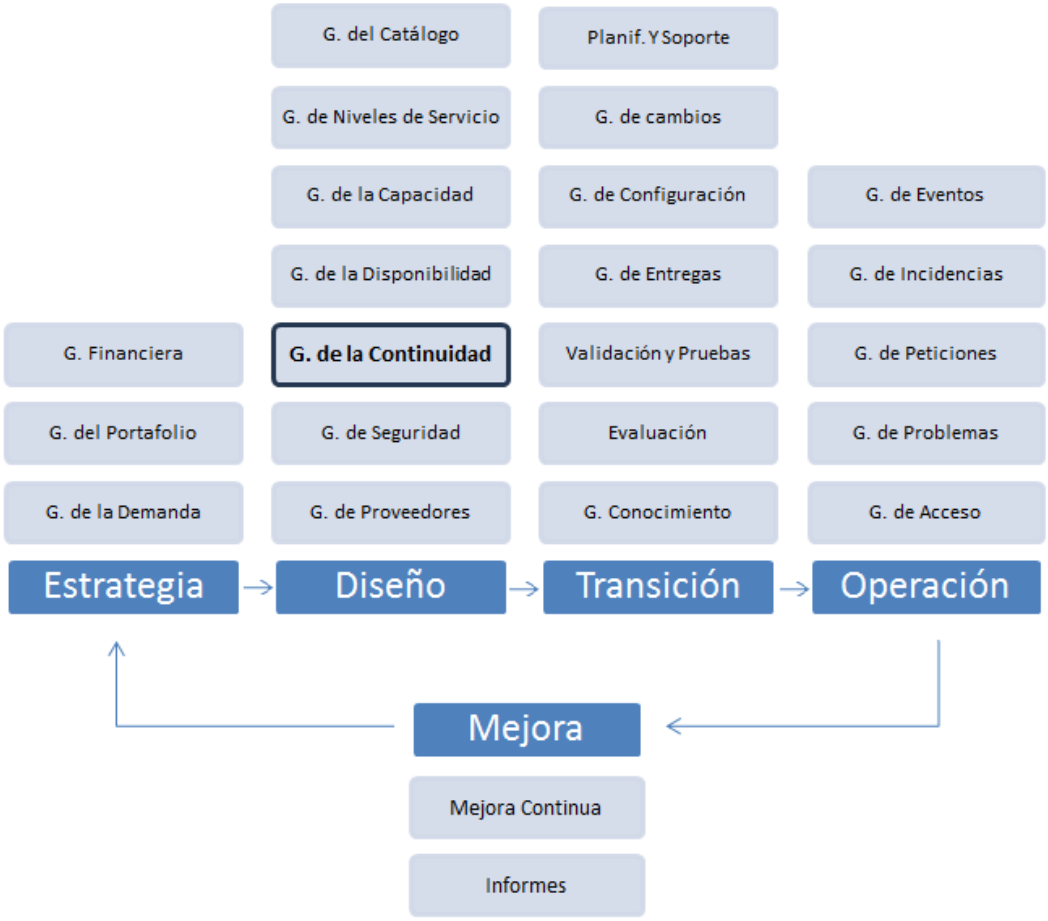


Figura 2. Procesos de la Gestión de Servicios de TI - ITIL

La **Gestión de la Continuidad del Servicio** se preocupa por impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tengan consecuencias catastróficas para el negocio.

Las siguientes secciones contienen detalles de cada una de las etapas en el ciclo de vida de ITSCM. [11]

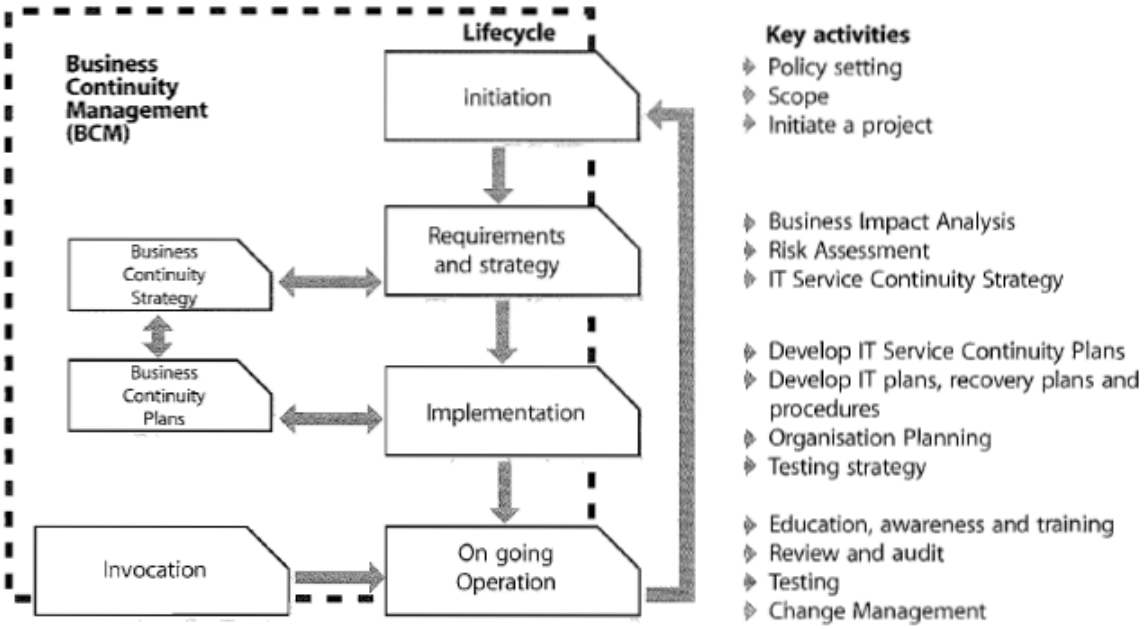


Figura 3. Ciclo de vida de la Gestión de la Continuidad de los Servicios
Fuente. ITIL v3 – Service Design

ETAPA 1 – INICIO

El proceso de iniciación cubre la totalidad de la organización y se compone de las siguientes actividades:

Configuración de Políticas. Debe ser establecido y comunicado tan pronto como sea posible para que todos los miembros de la organización involucrados o afectados por problemas de continuidad de negocio sean conscientes de sus responsabilidades para cumplir y apoyar ITSCM. Como mínimo, la política debe establecer la intención de la gestión y objetivos.

Especificar los términos de referencia y ámbito de aplicación. Incluye la definición del alcance y las responsabilidades de todo el personal de la organización. Abarca tareas como la realización de un Análisis de Riesgo y Análisis de impacto en las empresas y la determinación de la estructura de mando

y control necesarios para apoyar una interrupción del negocio. También es necesario tener en cuenta aspectos como los requisitos de los clientes, puntos pendientes de auditoría, reglamentaciones, condiciones de seguros y cumplimiento de las normas tales como ISO 27001 (que también se ocupa de los requisitos de continuidad de servicio).

Asignar recursos. El establecimiento de un eficaz medio de Continuidad de Negocio requiere recursos considerables en términos de dinero y mano de obra. Dependiendo de la madurez de la organización, con respecto a ITSCM, puede haber una obligación de conocer y/o capacitar al personal para llevar a cabo la Etapa 2. Como alternativa, el uso de consultores externos con experiencia puede ayudar a completar el análisis con mayor rapidez. Sin embargo, es importante que la organización pueda mantener el proceso en el futuro sin necesidad de depender totalmente de la ayuda externa.

Definir la organización del proyecto y la estructura de control. Los proyectos de ITSCM y BCM son potencialmente complejos y tienen que estar bien organizados y controlados. Se recomienda utilizar una reconocida metodología estándar de planificación del proyecto, PRICE o PMBOK.

Acuerdos del proyecto y planes de calidad. Los planes deben permitir que el proyecto sea controlado y administradas las desviaciones, asegurar que los servicios se consiguen en un nivel aceptable de calidad, proporcionar un mecanismo para comunicar las necesidades de recursos del proyecto y sus resultados finales, y así obtener la aprobación de todas las partes necesarias.

ETAPA 2 – REQUISITOS Y ESTRATEGIA

Conocer los requisitos de negocio para la continuidad del servicio es un componente crítico necesario para determinar qué tan bien la organización va a sobrevivir a un desastre o una interrupción y los costos en que se incurre. Si el análisis de los requisitos es incorrecto o la información clave ha sido perdida, podría tener graves consecuencias sobre la eficacia de los mecanismos de ITSCM. Esta etapa divide en dos secciones:

Requisitos – Análisis de impacto y evaluación de riesgos en la compañía.

Estrategia – Al realizar el análisis de los requisitos se establecen las medidas necesarias para reducir el riesgo y las estrategias de recuperación para apoyar el negocio.

Requisito – Análisis del impacto

El propósito de un Análisis de Impacto (BIA) es cuantificar el impacto que tendría el negocio debido a la pérdida de servicios. Este impacto podría ser un fuerte al ser identificado con exactitud, por ejemplo la pérdida financiera, o suave como las relaciones públicas, la salud moral y la seguridad o la pérdida de ventaja competitiva. En el BIA se identificarán los servicios más importantes para la organización y por lo tanto será el insumo clave para la estrategia.

El BIA identifica:

- El tipo de daño o pérdida, por ejemplo: pérdida de ingresos, costos adicionales, daño en la reputación, pérdida de ventaja competitiva, incumplimiento de la ley, pérdida a largo plazo de la cuota de mercado, pérdida de la capacidad operativa (en un entorno de mando o control).
- El grado o nivel de daño después de la interrupción del servicio, y las horas del día, semana, mes o año en que la interrupción será más grave.

- La dotación de personal, las habilidades, las instalaciones y servicios (incluidos los servicios de TI) necesarios para los procesos críticos de negocio puedan seguir operando a un nivel mínimo aceptable.
- El tiempo en el que los niveles mínimos de dotación de personal, instalaciones y servicios deben ser recuperados.
- El tiempo en el que todos los procesos de negocio necesarios y personal de apoyo, instalaciones y servicios debe estar plenamente recuperados.
- La prioridad relativa de recuperación para cada uno de los servicios de TI.

Requisito – Análisis de Riesgos

El propósito de un Análisis de Riesgos en ITSCM es determinar la probabilidad de que realmente ocurra un desastre o una interrupción grave de los servicios. Se trata de una evaluación del nivel de una amenaza y el grado en que una organización es vulnerable a ella. Puede utilizarse para evaluar y reducir la probabilidad de incidentes normales de funcionamiento. Se recomienda utilizar una metodología estándar de Administración de Riesgo.

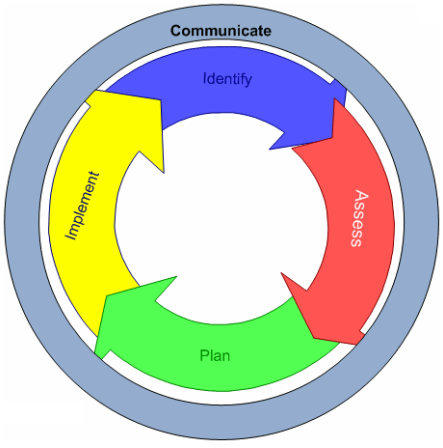


Figura 4. Proceso de Administración de Riesgos

Se deberá identificar las amenazas y oportunidades que podrían afectar la capacidad de alcanzar el objetivo de una actividad, evaluar el efecto neto de las amenazas detectadas y las oportunidades asociadas a una actividad, preparar una respuesta específica que reduzca las amenazas y maximizar las oportunidades, poner en práctica las acciones y supervisar su efectividad, tomar medidas correctivas cuando las respuestas no coinciden con las expectativas, revisar y mejorar las acciones para asegurar que siguen siendo eficaces, garantizar que todo el mundo se mantenga al día con los cambios en las amenazas, oportunidades y otros aspectos de la gestión de cualquier riesgo.

Estrategia – Continuidad

El resultado de los análisis de impacto y de riesgos permitirá definir estrategias de continuidad acordes con las necesidades del negocio. La estrategia deberá tener un equilibrio óptimo entre la reducción de riesgos, recuperación y opciones de continuidad. Se quiere concentrar los esfuerzos de reducción de riesgos en los servicios que han sido identificados como de alto impacto en el corto plazo dentro de BIA, por ejemplo, a través de la resistencia total y la tolerancia a fallos.

Opciones de Recuperación

La estrategia a seleccionar debe ser un equilibrio entre el costo de las medidas de reducción de riesgos y las opciones de recuperación para apoyar los procesos críticos de negocio dentro de los plazos acordados. La siguiente es una lista de las posibles opciones de recuperación de TI que necesitan ser considerados en el desarrollo de la estrategia:

- Trabajo Manual. Para ciertos tipos de servicios, puede ser una medida eficaz provisional durante un tiempo limitado hasta que el servicio de TI se reanude.

- Recuperación Gradual. Es llamada Cold standby, incluye la provisión de un sitio alterno vacío, totalmente equipado con electricidad, controles ambientales, infraestructura de red, cableado, conexiones de telecomunicaciones, y está disponible para la compañía en una situación de desastre para instalar su propio equipo informático. No incluye los equipos informáticos actuales, por lo que no es aplicable a los servicios que requieren pronta recuperación, esta opción sólo se recomienda para los servicios que puede soportar un retraso de tiempo de recuperación en días o semanas, no en horas.

- Recuperación Intermedia. Es llamada Warm standby, requiere un sitio alterno con sistemas activos diseñados para recuperar los servicios críticos en un plazo de entre 24 y 72 horas. La ventaja de esta opción es que el cliente puede tener acceso al sitio prácticamente al instante, ubicado en un edificio seguro, sin embargo, el restablecimiento de los servicios puede tomar algún tiempo, ya que los retrasos se pueden encontrar mientras se vuelve a configurar las aplicaciones y restaurar los datos de las copias de seguridad.

- Recuperación Rápida. Es llamada Hot standby, requiere un sitio alterno con una replicación continua de datos y con todos los sistemas activos preparados para la inmediata sustitución del ambiente de producción. Ésta es evidentemente la opción más costosa y debe emplearse sólo en el caso de que la interrupción del servicio TI tuviera inmediatas repercusiones comerciales. La instalación tiene que estar ubicada por separado y lo suficientemente lejos para no se vea afectado por una catástrofe que afecte a esa ubicación.

ETAPA 3 – IMPLEMENTACION

El Plan de ITSCM debe contener toda la información necesaria para recuperar los sistemas informáticos, redes y telecomunicaciones en una situación de desastre una vez presentada, y para gestionar el retorno al funcionamiento normal luego

que la interrupción del servicio se ha resuelto. Se debe elaborar una serie de documentos entre los que se incluyen:

- Plan de prevención de riesgos. Su objetivo principal es el de evitar o minimizar el impacto de un desastre en la infraestructura TI.

- Plan de gestión de emergencias. deben tener en cuenta aspectos como: evaluación del impacto de la contingencia en la infraestructura TI, asignación de funciones de emergencia al personal del servicio TI, comunicación a los usuarios y clientes de una grave interrupción o degradación del servicio, procedimientos de contacto y colaboración con los proveedores involucrados, protocolos para la puesta en marcha del plan de recuperación correspondiente.

- Plan de recuperación. Debe incluir todo lo necesario para: reorganizar al personal involucrado, restablecer los sistemas de hardware y software necesarios, recuperar los datos y reiniciar el servicio TI. Además, involucran: asignación de personal y recursos, instalaciones y hardware alternativos, Planes de seguridad que garanticen la integridad de los datos, procedimientos de recuperación de datos, Contratos de colaboración con otras organizaciones, Protocolos de comunicación con los clientes.

ETAPA 4 – OPERACIÓN EN CURSO

Esta etapa consistirá en lo siguiente:

- Educación, sensibilización y formación. Es indispensable que la ITSCM: dé a conocer al conjunto de la organización TI los planes de prevención y recuperación, ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación, realice periódicamente simulacros para

diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado, facilite el acceso permanente a toda la información necesaria.

- Revisión. Periódicamente revisar que todos los entregables del proceso ITSCM para asegurar que siguen siendo actuales.

- Pruebas. Es necesario establecer un programa de pruebas periódicas para garantizar que los componentes críticos de la estrategia se ponen a prueba, de preferencia al menos una vez al año, aunque las pruebas de Planes de Continuidad de Servicios de TI deben ser dispuestos de acuerdo con las necesidades del negocio y las necesidades de los BCP.

- Gestión de Cambios. Todos los planes también deben ser examinados después de cada cambio en los procesos principales. Cualquier cambio en la tecnología de TI también se debe incluir en la estrategia, para asegurar que después de un desastre funcione correctamente dentro de la prestación de servicios de TI.

- Invocación. Una interrupción puede ocurrir en cualquier momento del día o noche, por lo que es esencial que la guía del proceso de invocación esté disponible dentro y fuera de la oficina para el equipo de gestión de riegos. La decisión de invocar debe hacerse rápidamente para ahorrar tiempo en las habilitaciones de servicios en el sitio de recuperación, y no debe tomarse a la ligera si se va a utilizar un sitio de terceros por los costos y periodos determinados para el uso de las instalaciones. El período de retorno a la normalidad debe ser cuidadosamente planificado y realizado de manera controlada, es importante que todo el personal que sean consciente de sus responsabilidades para asegurar una transición sin problemas.

INDICADORES CLAVE DE RENDIMIENTO

KPI (Métrica de CSI)	Descripción
Procesos de negocio con acuerdos de continuidad	Porcentaje de procesos de negocio cubiertos por metas específicas de continuidad del servicio
Lagunas en preparación para desastres	Cantidad de lagunas identificadas en la preparación para eventos de desastres (amenazas serias sin contramedidas definidas)
Duración de la implementación	Duración desde la identificación del riesgo relacionado a desastres hasta la implementación de un mecanismo de continuidad adecuado
Cantidad de prácticas para desastres	Cantidad de prácticas para desastres que realmente se llevaron a cabo
Cantidad de defectos identificados durante las prácticas para desastres	Cantidad de defectos identificados en la preparación para eventos de desastres identificados durante las prácticas

4.4. COBIT

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). Permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas; constantemente se actualiza y armoniza con otros estándares, por lo tanto, se ha convertido en el integrador de las mejores prácticas de TI y marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. [10]

En COBIT se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que son: PLANEAR Y ORGANIZAR (PO), ADQUIRIR E IMPLEMENTAR (AI), ENTREGAR Y DAR SOPORTE (DS), MONITOREAR Y EVALUAR (ME).

El dominio ENTREGAR Y DAR SOPORTE cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. Dentro de este dominio se define el proceso DS11 - ADMINISTRACIÓN DE DATOS donde se tienen actividades que van desde la creación del marco de referencia para la continuidad de las operaciones y la definición de una estrategia y filosofía de continuidad hasta las indicaciones de contenido, implementación, prueba y distribución del mismo.

PROCESO DS11 - ADMINISTRACIÓN DE DATOS

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

Las entradas del proceso son:

Desde	Entradas
PO2	Diccionario de datos; clasificaciones de datos asignados
AI4	Manuales de usuario, de operación, de soporte, técnicos y de administración
DS1	OLAs
DS4	Plan de protección y de almacenamiento de respaldos

Figura 5. Entradas del Proceso DS11 – Administración de Datos
Fuente. Cobit 4.1

Las salidas del proceso son:

Salidas	Hacia
Reportes de desempeño del proceso	ME1
Instrucciones del operador para administración de datos	DS13

Figura 6. Salidas del Proceso DS11 – Administración de Datos
Fuente. Cobit 4.1

Los roles y responsabilidades para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso, son los siguientes:

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Traducir los requerimientos de almacenamiento y conservación a procedimientos				A	I	C	R				C
Definir, mantener e implementar procedimientos para administrar librerías de medios				A		R	C	C	I		C
Definir, mantener e implementar procedimientos para desechar de forma segura, medios y equipo				A	C	R			I		C
Respaldar los datos de acuerdo al esquema				A		R					
Definir, mantener e implementar procedimientos para restauración de datos				A	C	R	C	C			I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Figura 7. Matriz RACI del Proceso DS11 – Administración de Datos

Fuente. Cobit 4.1

OBJETIVOS DE CONTROL

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo, consisten en políticas, procedimientos, prácticas y estructuras organizacionales; están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

Los objetivos de control del proceso Administración de Datos son:

DS11.1 - Requerimientos del Negocio para Administración de Datos

Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio. Las necesidades de reinicio y reproceso están soportadas.

DS11.2 - Acuerdos de Almacenamiento y Conservación

Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.

DS11.3 - Sistema de Administración de Librerías de Medios

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS11.4 - Eliminación

Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

DS11.5 - Respaldo y Restauración

Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.

DS11.6 Requerimientos de Seguridad para la Administración de Datos

Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios.

METAS Y METRICAS

Es claro que los procesos requieren controles, los cuales son los que brindan la seguridad de que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Es así como para cada proceso se debe recoger información de control, la cual se debe comparar con una métrica y a partir del resultado se deberá actuar para obtener el mayor beneficio.

Se definen en COBIT en tres niveles:

- Las metas y las métricas de TI, que definen lo que el negocio espera de TI.
- Las metas y las métricas de Procesos, que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI.
- Las metas y las métricas de las Actividades, que facilitan el desempeño efectivo de los procesos.

Las metas y las métricas del Proceso DS11 - ADMINISTRACIÓN DE DATOS, se detallan en la siguiente tabla:

	TI	PROCESOS	ACTIVIDADES
METAS	- Optimizar el uso de información. - Garantizar que la información crítica y confidencial se mantiene oculta contra quienes no deben tener acceso a ella. - Garantizar que TI cumpla con las leyes y regulaciones.	- Mantener la completitud, exactitud, validez y accesibilidad de los datos almacenados. - Asegurar los datos durante el desecho de medios. - Administrar de manera efectiva el almacenamiento de medios.	- Respaldo de datos y prueba de restauración. - Administración de almacenamiento de datos en sitio y fuera del sitio. - Desecho seguro de datos y equipo.

METRICAS	- Número de eventos donde se presente incapacidad para recuperar información crítica para el proceso de negocio. - Satisfacción del usuario con la disponibilidad de la información. - Incidentes de incumplimiento de las leyes debido a problemas con la administración del almacenamiento.	- % de restauraciones de datos exitosas. - # de incidentes en los que se recuperaron datos de medios y equipos ya desechados. - # de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento.	- Frecuencia de las prueba de los medios de respaldo. - Tiempo promedio del tiempo de restauración de datos.

Fuente. Cobit 4.1

MODELO DE MADUREZ

Los modelos de madurez ayudan a los directivos de las organizaciones a identificar que tan bien se está administrando TI, es un método que permite evaluar desde un nivel 0-No existente hasta el nivel 5-Optimizado. En él se podrá identificar: el desempeño real de la empresa, el estatus actual de la industria y el objetivo de mejora de la empresa.

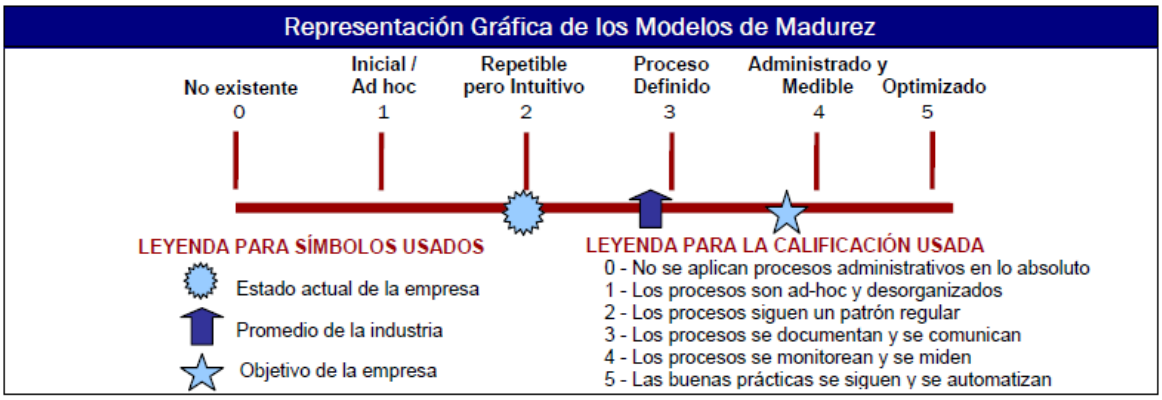


Figura 8. Modelo de Madurez del Proceso DS4 – Garantizar la Continuidad del Servicio
Fuente. Cobit 4.1

EL modelo de madurez del proceso Garantizar la Continuidad del Servicio es:

0 - No Existente

Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.

1 - Inicial / Ad Hoc

La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo habilitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.

2 - Repetible pero Intuitivo

A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.

3 - Definido

Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo. Se lleva a cabo algún tipo de monitoreo sobre la administración de datos. Se definen métricas básicas de desempeño. Comienza a aparecer el entrenamiento sobre administración de información

4 - Administrado y Medible

Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de

desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.

5 - Optimizado

Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente, la compartición del conocimiento es una práctica estándar. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se acuerdan con los clientes los indicadores de desempeño y meta, se ligan con los objetivos del negocio y se monitorean de manera regular utilizando un proceso bien definido. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.

5. ALCANCES Y LIMITACIONES

Los alcances de este proyecto consisten básicamente en lograr diseñar un Marco Metodológico para la implementación de una estrategia de respaldo y copias de seguridad, que incluye las fases de Diagnóstico, Diseño y presentación del Marco. Este proyecto no abarca la implementación del marco metodológico, pero se van incluir ejemplos y procesos claves que ilustren la estructura del plan.

6. METODOLOGIA

El marco metodológico se desarrollará haciendo un recorrido detallado del estándar BS 25999, el proceso Gestión de la Continuidad de los Servicios de TI de ITIL y el proceso “DS4 - Asegurar la continuidad del servicio” del dominio “Entrega y soporte” de COBIT; con el propósito de precisar e identificar las áreas y fases a tratar en el marco metodológico a proponer. Después de esto, consideramos que para cumplir con los objetivos o dar respuesta concreta al problema identificado se deben aplicar la investigación, observación, análisis y síntesis en las siguientes etapas:

Etapa 1: Interpretación de los diferentes estándares. Consiste en la lectura, análisis y síntesis de BS - 25999, ITIL y COBIT. En este caso se realizará una seria investigación y levantamiento de información adicional que permita el - entendimiento de los Procesos**.**

Etapa 2: Formulación del proyecto. Consistirá en la definición y detalle de las metas en tiempo, espacio, objetivos y alcances.

Etapa 3: Definición de un marco metodológico compuesto por diferentes fases y actividades. Consistirá en la identificación de las principales fases y actividades, y determinar las herramientas que se necesitarán para seguir las pautas del marco de trabajo.

Etapa 4: Diseño de la Herramienta. En esta etapa se realizará el diseño de la herramienta, teniendo en cuenta las fases y actividades de un Plan de Continuidad del Negocio.

7. IMPACTOS Y RESULTADOS ESPERADOS

Este proyecto surge como una necesidad del sector empresarial, y proporcionará un marco metodológico o una guía práctica para que el personal de TI, implemente de manera ágil un Plan de Continuidad del Negocio que permita prevenir o evitar los posibles escenarios originados por una situación de crisis así como minimizar las consecuencias económicas, reputacionales o de responsabilidad civil derivadas de la misma, y que ayude a reducir los costos asociados a la interrupción o evitar penalizaciones contractuales por incumplimiento de contratos como proveedor de productos o servicios.

8. MARCO METODOLÓGICO PROPUESTO

En primera instancia una representación gráfica de las fases que componen el marco metodológico para el desarrollo de un Plan de Continuidad propuesto en el cual se distinguen 7 fases secuenciales que son:

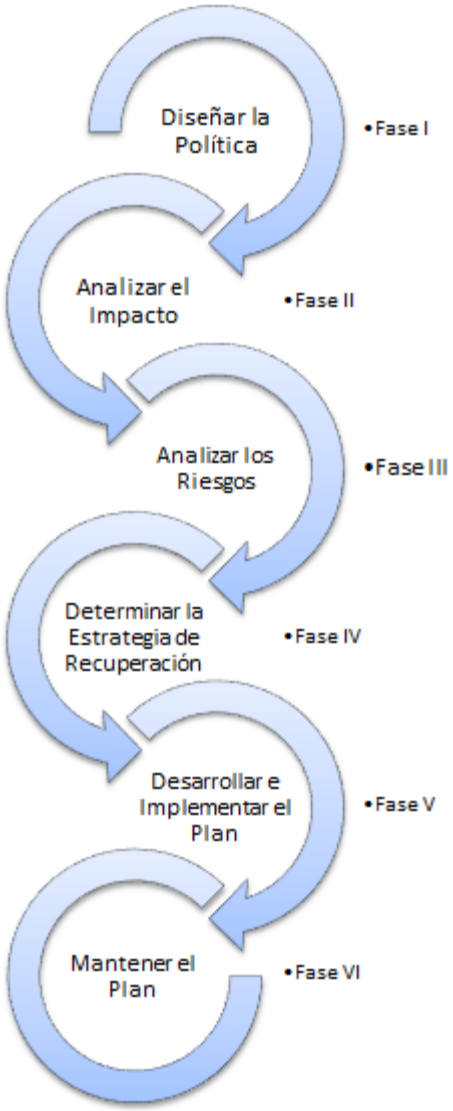


Figura 9. Diagrama de Fases del Plan de Continuidad

BIBLIOGRAFIA

Emergency Management Forum, 2001. Documentación en línea: http://www.oakridge.doe.gov/external/Home/PublicActivities/EmergencyManagementForum/tabid/307/Default.aspx

GASPAR J., 2004. Planes De Contingencia. La Continuidad Del Negocio En Las Organizaciones.

BS – 25999, Sep – 2010. British Standard – 25999. Documentación en línea: http://www.bs25999.com/

ITIL, Sep – 2010. Information Technology Infrastructure Library. Documentación en línea: http://www.itil-officialsite.com/home/home.asp

ISACA, Sep – 2010. COBIT. Control Objectives for Information and related Technology. Documentación en línea: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Bon J., Ene – 2008. Fundamentos de la Gestión de Servicios de TI basada en ITIL V3. Van Haren Publishing, Tercera Edición. Cap 2, pág. 10.

BCI – 2007. Bussines Continuity Institute: Manual de Buenas Prácticas. Traducido por ISMS Forum Spain. Pág. 12 – 13.

BS – 25999-1, 2006. Bussines Continuity Managemente, Part 1. Code of Practice. Pág. 12 – 47.

SkillSoft Corporation – 2007. Managing Infrastructure using ITIL.

Texto: ITIL v3 - “Service Design”, 2007. Publicado por Office of Government Commerce. Pág. 125 – 155.

IT Governance Institute, 2010. COBIT 4.1. Pág. 120 – 123.

ANEXOS

ESQUEMAS TRADICIONALES DE REALIZACION DE BACK-UP Y RESPALDO DE INFORMACION.

1. **ESQUEMA DE RESPALDO DE INFORMACION CON UNA HERRAMIENTA HARDWARE – SOFWARE (TIVOLI).**

1. INFORMACIÓN GENERAL

1.1 OBJETIVO	Garantizar la disponibilidad, seguridad y confidencialidad de la información Institucional de la Entidad mediante la gestión de las copias de respaldo y su recuperación cuando sea requerido
1.2. RESPONSABLE	Coordinador Grupo de Sistemas
1.3. ALCANCE	Realizar el respaldo de información institucional almacenada en los equipos ubicados en el centro de cómputo de la Superintendencia de Sociedades en la ciudad de Bogotá D.C. y la administración y custodia de las cintas o medios de respaldo que se generen de este ejercicio, bien sea que se encuentren en la Entidad o se entreguen en custodia externa.
1.4. DEFINICIONES	**Sistema Operativo:** Programa o conjunto de programas que actúan como intermediarios entre las aplicaciones de los usuarios (Software) y el equipo físico (Hardware) de la máquina, ocultando las características particulares de este último. **Aplicaciones:** Nombre que reciben los programas especializados en tareas concretas y de una cierta complejidad **Bases de Datos:** Es la colección de información, que está organizada de forma tal que su contenido sea fácilmente accedido, administrado y actualizado. **Custodia:** Se entrega al cuidado de una persona natural o jurídica. **Librería de cintas de Backups (Tape Library):** Dispositivo de Hardware que realiza la rutina de respaldo en cintas de manera automática **Respaldo:** Sinónimo de backup. **Backup:** Copia idéntica de algo, copia de seguridad o copia respaldo de algo. **TSM:** Tivoli Storage Manager- herramienta tipo software de gestión de backups, que permite programar y realizar de forma automática los backups.

2. CONDICIONES GENERALES

2.1. Es responsabilidad de los líderes de procesos y jefes de dependencias garantizar que la información institucional sea almacenada y respaldada en la infraestructura de la Entidad; para esto debe solicitar la creación de un sitio de almacenamiento digital con sus correspondientes carpetas, indicando que funcionarios tienen control, los niveles de acceso, clasificación, la seguridad y tiempo de retención, además de garantizar que los responsables de los datos los depositen y/o actualicen en las carpetas asignadas.

2.2. No se podrá almacenar en el centro de cómputo de la Entidad información de índole personal o que no corresponda a la legalmente autorizada, cumpliendo con la normatividad relacionada con derechos de autor.

2.3. Identificar claramente la información crítica que se debe respaldar, indicando los niveles de seguridad e incluir las condiciones necesarias para futuras restauraciones.

2.4. Aplicar a la información los siguientes criterios de respaldo:

NIVEL REQUERIDO	GRADO DE BACKUP	FRECUENCIA
Sistema operativo, Aplicaciones, Bases de datos, Servidor, File Systems, etc	Parcial Completo Incremental	Mensual Semanal, Diario,

2.5. Garantizar con el Almacén de la Entidad la disponibilidad de las cintas de backup requeridas de acuerdo con la cantidad de información estimada a almacenar.

2.6. Garantizar la custodia y almacenamiento de los medios con una Empresa Externa Especializada de acuerdo con los compromisos del y la vigencia del contrato.

2.7. Las cintas que son retiradas de la librería de cintas de backup deben ser estar ubicadas en un área con las medidas de seguridad necesarias antes de ser entregadas a la empresa de custodia externa o al usuario responsable de la información.

2.8. Monitorear regularmente los registros de logs y eventos de las herramientas, junto con los procedimientos de los backups realizados. En caso de encontrar alguna alarma o sospecha de la calidad del backup, se debe repetir y hacer seguimiento para corregir las fallas detectadas.

2.9. El responsable de las copias de seguridad con el líder de seguridad, deben realizar trimestralmente pruebas de recuperación y calidad de la información de manera aleatoria, y dejar registro a través de un incidente en la mesa de ayuda o en caso de no existir sistema mediante acta.

2.10. Se aplicará los mismos criterios de respaldo a la información Institucional que sea almacenada en los medios de almacenamiento destinados para ello, cuando no se encuentre automatizado el proceso, para lo cual el Coordinador de Sistemas establecerá y aplicará estos mecanismos, dejando igualmente constancia a través de la mesa de ayuda.

2.11. Cuando se presenten cambios del ambiente productivo y dependiendo de los recursos disponibles se debe contemplar la actualización de la parametrización de la librería de respaldo y la inclusión dentro de los mecanismos de respaldo disponibles.

2.12. Las cintas de respaldo serán identificadas conforme lo permite la librería de backup y en otros mecanismos de respaldo se deberán identificar con el contenido y fecha de realización, al igual con el número de veces que ha sido usado el mecanismo.

3. *DESCRIPCION DE LA ACTIVIDAD*

Flujograma	Descripción	Responsable	Documentos o formatos	Puntos de control
	Inicio			
	Solicitar la creación del sitio de almacenamiento, indicando los niveles de acceso, clasificación, seguridad y tiempo de retención, además serán responsables de depositarla en las carpetas asignadas.	Líderes de los procesos y Jefes de Dependencia	Mesa de ayuda	
	Evaluar, aprobar y comunicar la decisión sobre la solicitud de respaldo de información institucional.	Líder Centro de Cómputo o el líder de Soporte técnico		
	Preparar, evaluar y aprobar la solicitud de cambio al ambiente productivo, según el procedimiento GINF_PR-006.	Líder Centro de Cómputo y Coordinador Grupo de Sistemas		
	Aplicar el plan de cambio al ambiente productivo para incorporar la solicitud de respaldo de información institucional.	Líder del Centro de Cómputo	Aplicativo o mesa de ayuda	
	Verificar la disponibilidad, calidad y espacio en las cintas donde se realizarán los respaldos.	Líder del Centro de Cómputo	Aplicativo o mesa de ayuda	
	Ejecutar las copias de respaldo de la información Institucional del centro de cómputo.	Líder del Centro de Cómputo o personal autorizado	Aplicativo o mesa de ayuda	
	Identificar, preparar, almacenar y entregar para la custodia de las cintas de la librería de respaldo TSM.	Funcionarios autorizados de la Entidad.		
	Fin			

4. ANEXOS Y REGISTROS

Aplicativo **TSM** Tivoli Storage Manager
Mesa de Ayuda

5. CONTROL DE CAMBIOS.

Versión	Vigencia Desde	Vigencia Hasta	Identificación de los cambios	Responsable
001	23-12-08	14-07-2010	Creación del documento	Líder Centro de Cómputo
002	14-07-2010	11-05-2011	Inclusión de Condiciones Generales 2.2.	Líder Centro de Computo
003	12-05-2011		Ajuste del procedimiento de acuerdo con la política de respaldo y recuperación.	Coordinador de Sistemas

2. ESQUEMA DE RESPALDO Y RESTAURACION DE LA INFORMACION CON MEDIOS MAGNETICOS Y UNIDADES TRADICIONALES.

1. OBJETIVO

Proteger la información, base de datos y documentación crítica para la entidad con el fin que se conserven respaldados, así como la restauración de la misma en el momento que se necesite.

2. ALCANCE

Inicia con la programación que se tiene definida en el área de sistemas para las copias de seguridad de la información y bases de datos y termina con la verificación del backup y la salvaguardia de la información.

3. INSUMOS

Bases de datos (Orfeo), aplicativos, plataformas, solicitudes.

4. PRODUCTOS Y/O INFORMACIÓN SECUNDARIA

Información en medios magnéticos y discos, bitácora de control de backup.

5. NORMAS O REQUISITOS LEGALES

Consultar normograma.

6. TÉRMINOS Y DEFINICIONES

Archivos log: Es un registro oficial de eventos durante un rango de tiempo en particular, es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (Who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

Backup o copia de seguridad: es la acción de copiar archivos de forma total o parcial de la información archivos, carpetas aplicaciones o bases de datos, esta copia de respaldo debe ser guardada en cd, DVD, Discos Duros o cintas.

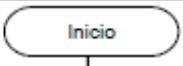
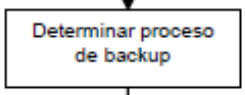
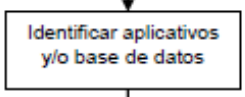
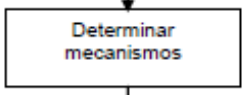
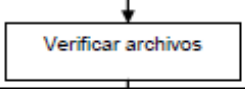
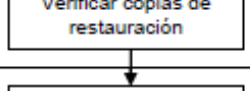
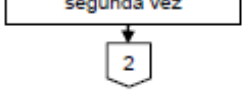
Bases de datos: Conjunto de datos perteneciente a un mismo contexto almacenados sistemáticamente.

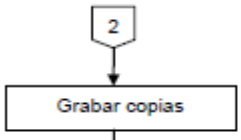
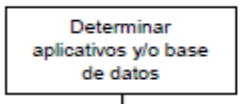
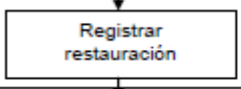
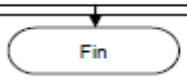
DVD (Disco versátil Digital): Disco óptico de almacenamiento de datos que pueden ser de lectura R o lectura escritura RW.

7. CONDICIONES GENERALES

- El responsable de sistemas debe definir y dar cumplimiento a la política de backup de la entidad.
- Una vez el funcionario se retire de la entidad, el ingeniero de sistemas debe dejar registro del backup realizado mediante el formato establecido.

8. DESCRIPCIÓN DEL PROCEDIMIENTO

Nº	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable	Documento o Registro
Realización de Backup				
		Inicio del procedimiento		
1		Se determinan e identifican los archivos a respaldar en los equipos en las diferentes áreas.	Ing. Sistemas o Ing. Soporte	
2		Se identifica el número de aplicativos y/o bases de datos para respaldo.	Ing. Sistemas o Ing. Soporte	Inventario de aplicativos
3		Se determinan los mecanismos de copias de respaldo según la base de datos a respaldar de forma manual.	Ing. Sistemas o Ing. Soporte	Bitácora de backup
4		Se verifican los archivos log del aplicativo utilizado para la copia de seguridad.	Ing. Sistemas o Ing. Soporte	
5		Se verifican las copias para la restauración cuando se necesiten por cualquier usuario de la entidad.	Ing. Sistemas o Ing. Soporte	
6		Si el archivo log del servidor indica un error, se realiza copia por segunda vez.	Ing. Sistemas o Ing. Soporte	

Nº	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable	Documento o Registro
7		Se graba de manera diaria, semanal, mensual y anualmente de acuerdo con la política de backup, en un dispositivo de almacenamiento (Servidor o Disco Externo) todas las copias y guardar en área de sistemas.	Ing. Sistemas o Ing. Soporte	
8		Se almacena la copia, y para el caso de ser un medio magnético (CD y/o DVD) se marca con la respectiva fecha, usuario y nombre del equipo.	Ing. Sistemas o Ing. Soporte	Formato backups
		Fin del procedimiento		
Restauración				
1		Se determina o identifica el número de aplicativos y/o bases de datos para la restauración.	Ing. Sistemas o Ing. Soporte	
2		Se realiza la restauración de los archivos correspondientes en el equipo del usuario. Si es una base de datos (en el caso de Orfeo), se determina la hora para la respectiva restauración y se informa a los usuarios para suspender el aplicativo mientras se realiza la respectiva reposición.	Ing. Sistemas o Ing. Soporte	
3		Se registra la restauración realizada, si es una base de datos se guarda el registro o bitácora del mismo.	Ing. Sistemas o Ing. Soporte	Bitácora backups
		Fin del procedimiento		

9. CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Cambios realizados
0	23 de Abril de 2013	Documento original.

10. APROBACIÓN

Elaboró y Validó	Apoyó y Revisó	Aprobó
LUIS CORTÉS CASTIBLANCO Profesional Universitario **SUBDIRECCIÓN DE GESTIÓN CORPORATIVA** -Documento original firmado en Subdirección General-	CATHERINE CIFUENTES GUERRERO Profesional Contratista **SUBDIRECCIÓN GENERAL** -Documento original firmado en Subdirección General-	ALFREDO JOSÉ DELGADO DÁVILA Subdirector de Gestión Corporativa **SUBDIRECCIÓN DE GESTIÓN CORPORATIVA** -Documento original firmado en Subdirección General-
Fecha: 16 de octubre de 2012	**Fecha:** 17 de octubre de 2012	**Fecha:** 23 de Abril de 2013

3. TIPOS DE COPIAS DE SEGURIDAD Y RESPALDO DE INFORMACION y DESCRIPCION DE LA ESTRATEGIA DE BACK-UP DE UNA EMPRESA CONTACT CENTER.

4.1.1. Tipos de respaldo de información

4.1.1.1. Copia de seguridad completa

Copia de seguridad completa es el punto de partida para el resto de las copias de

[5] SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. TÜV SÜD Iberia, S.L.U. España. 2012. C/Frederic Mompou 8 p [en linea].] [Consultado 15-03-2013] Disponible en web: < http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039-iso-iec-27001-es-260412.pdf >

[6] NTP-ISO/IEC Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información 27001. Primera edición. [en línea]. 2008-12-12 [Consultado 15-03-2013] Disponible en web: <http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf>

[7] Ibíd., p. 3

[8] IBM. Infraestructura de la información. [en línea]. Disponible en web: <http://www-03.ibm.com/systems/es/information_infrastructure/solutions/information_availability/>[Consultado 15-03-2013]

seguridad y contiene todos los datos de las carpetas y los archivos que se han seleccionado para la copia de seguridad. Debido a que la copia de seguridad completa almacena todos los archivos y carpetas, copias de seguridad completas frecuentes resultan en operaciones de restauración más rápida y más simple. Recuerde que cuando se elige otro tipo de copia de seguridad, tareas de restauración pueden tardar más tiempo.

Sería ideal para hacer copias de seguridad completas todo el tiempo, ya que son los más completos y son auto-contenida. Sin embargo, la cantidad de tiempo que se necesita para ejecutar copias de seguridad completas a menudo nos impide utilizar este tipo de copia de seguridad. Copias de seguridad completas a menudo se limitan a un horario semanal o mensual, aunque el aumento de la velocidad y la capacidad de los medios de copia de seguridad están haciendo copias de seguridad completas durante la noche una propuesta más realista.

Copias de seguridad completas ofrecen la mejor solución en protección de datos y teniendo en cuenta que se puede programar una copia de seguridad para que se ejecute automáticamente, requiere poca intervención en comparación con los beneficios. Una sola copia de seguridad completa proporciona la capacidad de restaurar completamente todos los archivos y carpetas de la copia de seguridad, como se ejemplifica en la siguiente imagen:

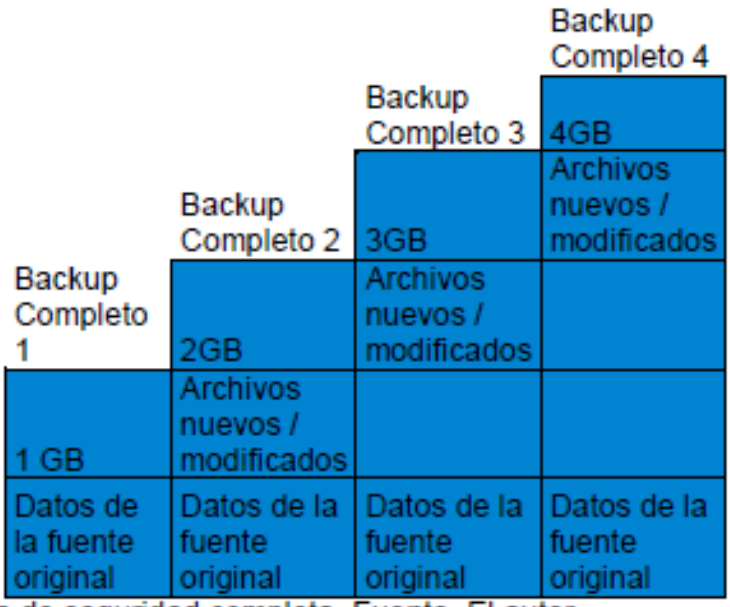


Figura 1. Copia de seguridad completa. Fuente. El autor

Sin embargo, debe ser consciente de un problema de seguridad importante: cada copia de seguridad completa contiene una copia completa de los datos. Si los medios de copia de seguridad debían ser visitada, robados o perdidos ilegalmente, toda la copia de sus datos podría estar en manos de personas no autorizadas. Por eso, cuando la decisión de utilizar un programa de copia de seguridad para realizar copias de seguridad completas, asegúrese de que es compatible con el cifrado para proteger los datos de copia de seguridad.

Tabla 1. Ventajas y desventajas copia de seguridad completa. Fuente. Backup4all

Las ventajas	**Las desventajas**
• Restaurar es el más rápido • Los datos de copia de seguridad de todo se almacena en un único archivo (mejor gestión de almacenamiento)	• Copia de seguridad es el más lento en comparación con otros tipos de copia de seguridad • Los requisitos de espacio de almacenamiento son los más altos (en comparación con copia de seguridad incremental o de copia de seguridad diferencial). Teniendo en cuenta cómo los dispositivos de almacenamiento baratos están ahora, esto es una desventaja de bajo impacto.

Como recomendación, aunque llena de copia de seguridad ofrece la mejor protección, es bueno contar con una estrategia de copia de seguridad en el lugar donde se realizan copias de seguridad completas semanales, y los tipos de copia de seguridad más rápidas (como incremental) se ejecutan diariamente. [9]

4.1.1.2. Copia de seguridad incremental

Copia de seguridad incremental almacena todos los archivos modificados desde el último respaldo completo, diferencial o copia de seguridad incremental. La ventaja de una copia de seguridad incremental es que se tarda menos tiempo para terminar. La desventaja es que, durante una operación de restauración, cada incremento se procesa, lo que podría resultar en una tarea de restauración largo.

Copia de seguridad incremental proporciona un método más rápido de copia de seguridad de datos que se ejecuta repetidamente copias de seguridad completas. Durante una copia de seguridad incremental, sólo los archivos modificados desde la última copia de seguridad se incluyen. Ahí es donde se pone su nombre: cada

[9] Backup4all. full backup. 2011. [En línea]. Disponible en web: <,http://www.backup4all.com/kb/full-backup-116.html>[Consultado 15-03-2013]

copia de seguridad es un incremento de una copia de seguridad anterior.

La representación siguiente muestra cómo un trabajo de copia de seguridad se ejecuta cuatro veces parecería al utilizar incrementales:

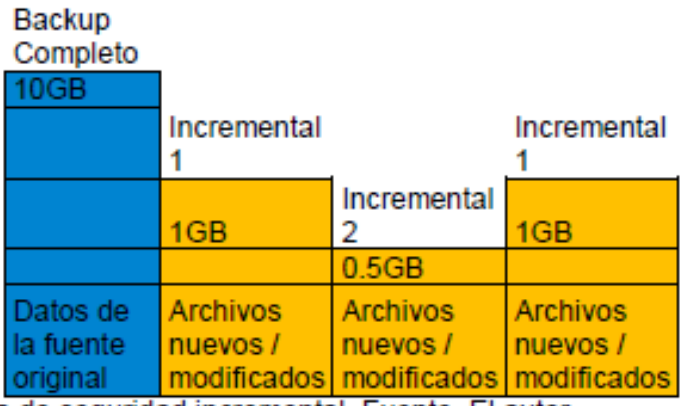


Figura 2. Copia de seguridad incremental. Fuente. El autor

El tiempo que se tarda en ejecutar la copia de seguridad puede ser una fracción del tiempo que se tarda en realizar una copia de seguridad completa. Backup4all es un programa de copia de seguridad que admite copias de seguridad incrementales, y utiliza la información registrada en su archivo de catálogo (. BKC) para determinar si cada archivo ha cambiado desde la última copia de seguridad.

La ventaja de los tiempos de copia de seguridad más bajos tiene un precio: aumentado el tiempo de restauración. Al restaurar desde copia de seguridad incremental, se necesita el respaldo completo más reciente, así como cada copia de seguridad incremental que ha realizado desde la última copia de seguridad completa.

Por ejemplo, supongamos que usted hizo una copia de seguridad completa el viernes y copias de seguridad incrementales de lunes, martes y miércoles. Si tiene que restaurar la copia de seguridad el jueves por la mañana, usted necesitaría los cuatro archivos contenedores de copia de seguridad: copia de seguridad completa del viernes, además de la copia de seguridad incremental para el lunes, martes y miércoles. En comparación, si hubieras ejecutar copia de seguridad diferencial el lunes, martes y miércoles, luego de restaurar el jueves por la mañana que habría necesitado sólo del viernes copia de seguridad completa más el diferencial del miércoles.[10]

[10] Backup4all. Incremental backup. 2011. [En línea]. Disponible en web: <http://www.backup4all.com/kb/incremental-backup-118.html >[Consultado 15-03-2013]

Tabla 2. Ventajas y desventajas copia de seguridad incremental. Fuente. Backup4all

Las ventajas	Las desventajas
Es el tipo de copia de seguridad más rápido, ya que sólo realiza copias de incrementos-up. Ahorra espacio de almacenamiento en comparación con otros tipos. Cada incremento de copia de seguridad puede almacenar una versión diferente de un archivo / carpeta.	Restauración completa es lento en comparación con otros tipos de copia de seguridad (es necesario la primera copia de seguridad completa y todos los incrementos desde entonces). Para restaurar la última versión de un archivo individual el incremento que lo contiene se debe encontrar primero.

4.1.1.3. Copia de seguridad diferencial

Copia de seguridad diferencial contiene todos los archivos que han cambiado desde la última copia de seguridad completa. La ventaja de una copia de seguridad diferencial es que se acorta el tiempo de restauración en comparación con una copia de seguridad completa o una copia de seguridad incremental. Sin embargo, si se realiza la copia de seguridad diferencial demasiadas veces, el tamaño de la copia de seguridad diferencial podría llegar a ser más grande que la copia de seguridad completa inicial.

Existe una diferencia significativa, pero a veces confusa, entre copia de seguridad diferencial y copias de seguridad incrementales. Mientras espalda incremental de seguridad de todos los archivos modificados desde la última copia de seguridad completa, diferencial o copia de seguridad incremental, copia de seguridad diferencial ofrece un término medio de copia de seguridad de todos los archivos que han cambiado desde la última copia de seguridad completa. Ahí es donde se pone su nombre: realiza copias de seguridad todo lo que es diferente desde la última copia de seguridad completa.

En la siguiente imagen se puede ver un ejemplo de cómo una copia de seguridad diferencial se vería como un trabajo de copia de seguridad que se ejecuta cuatro veces:

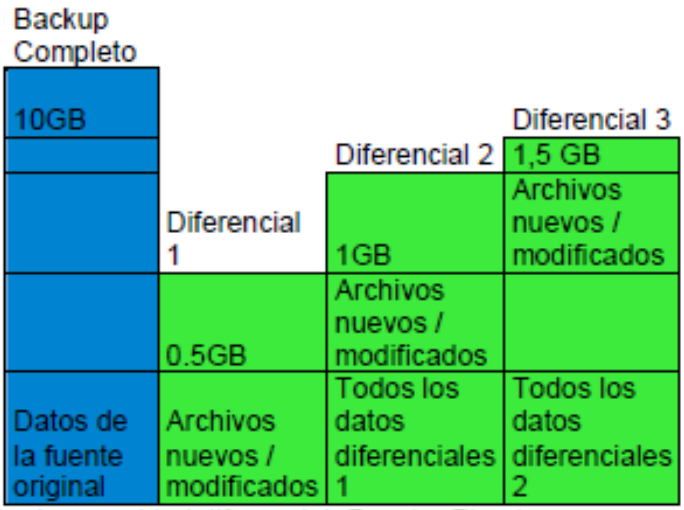


Figura 3. Copia de seguridad diferencial. Fuente. El autor

Restaurar una copia de seguridad diferencial es un proceso más rápido que la restauración de una copia de seguridad incremental, porque sólo se necesitan dos archivos de copia de seguridad de contenedor: la última copia de seguridad completa y la última diferencial.

Restaurar una copia de seguridad diferencial es un proceso más rápido que la restauración de una copia de seguridad incremental, porque sólo se necesitan dos archivos de copia de seguridad de contenedor: la última copia de seguridad completa y la última diferencial.

Utilice copia de seguridad diferencial si usted tiene una cantidad razonable de tiempo para realizar copias de seguridad. La ventaja es que sólo se necesitan dos archivos contenedores de copia de seguridad para realizar una restauración completa. El inconveniente es que si se ejecutan varias copias de seguridad diferenciales después de la copia de seguridad completa, probablemente incluyendo algunos archivos en cada copia de seguridad diferencial que ya se incluyeron en las copias de seguridad diferenciales anteriores, pero no han sido modificadas recientemente.

Tabla 3. Ventajas y desventajas copia de seguridad diferencial. Fuente. Backup4all

Ventajas	Desventajas
Restaurar es más rápida que la restauración de copia de seguridad incremental.	Restaurar es más lenta que la restauración de copia de seguridad completa.
Copia de seguridad es más rápido que una copia de seguridad completa.	Copia de seguridad es más lento que copia de seguridad incremental.

La buena implementación de los anteriores tipos de backup es necesaria para tener en la organización la información disponible e integra la cual reposa en los servidores que maneja la empresa.[11]

4.1.2. Servidores que se tienen actualmente en la empresa

Un servidor es un dispositivo que forma parte de una red el cual distribuye o proporciona algún servicio a un cliente. Los servidores que se disponen tienen cada uno un rol específico dentro de la compañía y se explican a continuación:

Servidor de archivos: almacena varios tipos de archivo y los distribuye a otros clientes en la red.[12]

Servidor de correo electrónico: almacena, envía, recibe, en ruta y realiza otras operaciones relacionadas con e-mail para los clientes de la red.[13]

Servidor de aplicaciones: Aloja las aplicaciones internas de la compañía. Cumple la función de proporcionar funciones a equipos clientes.

Servidor de base de datos: Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.[14]

Servidor de dominio: servidor que permite centralizar el trabajo de los usuarios de la red, sus archivos, configuraciones y perfiles, en un solo ordenador, y permite el acceso a ellos desde cualquier ordenador de la red de forma segura.[15]

Servidor de impresión: controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión (aunque también puede cambiar la prioridad de las diferentes impresiones), y realizando la mayoría o todas las otras funciones que en un sitio de trabajo se realizaría para lograr una tarea de impresión si la impresora fuera conectada

---

[11] Backup4all. differential backup. 2011. [En línea]. Disponible en web: < http://www.backup4all.com/kb/differential-backup-117.html>[Consultado 15-03-2013]

[12] Bermeo Aucay, Freddy Rafael. Análisis De La Seguridad Física Del Servidor Y Backup De Base De Datos, En La Cooperativa Jardín Azuayo. Director: Ing. Marco Litúma. Cooperativa jardín azuayo. Cuenca – Ecuador. 2011

[13] Ibid,p. 11.

[14] Ibid, p. 11.

[15] Servicios informáticos. Servidor de archivos y dominio [En línea]. Disponible en web: <http://www.serinformaticos.es/?file=kop404.php> [Consultado 15-03-2013]

directamente con el puerto de impresora del sitio de trabajo.[16]

Servidor web: la función que cumple es almacenar los archivos de un sitio y emitirlos por Internet para poder ser visitado por los usuarios.[17]

Servidor antivirus: ayuda a impedir el paso a los hackers, virus y gusanos que intenten entrar en los equipos a través de Internet.[18]

La empresa de contact center desarrolla sus actividades en sector de mercado de BPO; donde se comercializan productos y servicios de terceros a través de outsoursing en el área de telemercadeo.

Siendo así para que una empresa de contact center trabaje en estos nichos de mercado es necesaria la utilización de tecnologías de vanguardia que permitan monitorear y evidenciar el contacto con el cliente, para ello las entidades certificadoras aconseja utilizar diferentes plataformas avaladas por los estándares de calidad en el área de contact center. Como CCA desarrollado por ORACLE que permite administrar las relaciones con el cliente.

Actualmente la empresa cuenta con la información centralizada donde cada cliente almacena información en un espacio dedicado para el desarrollo de su actividad. Adicionalmente el software manejado por la empresa, graba de manera continua todas las llamadas generadas de entrada y salida (inbound and outbound), para todas las líneas de negocio. Ya que la empresa actualmente maneja un mediano volumen de información, es importante la realización de copias de seguridad de la información que posea la compañía.

Un aspecto que es interesante señalar en cuanto al uso de las mejores prácticas en respaldo y aseguramiento de la información, dato brindado por la Cámara de Comercio de Londres: "El 90% de las empresas que sufren una pérdida de datos importante desaparece del mercado en dos años."[19] Asunto que es importante

---

[16] BERMEO AUCAY, Freddy Rafael. Análisis De La Seguridad Física Del Servidor Y Backup De Base De Datos, En La Cooperativa Jardín Azuayo. Director: Ing. Marco Litúma. Cooperativa jardín azuayo. Cuenca – Ecuador. 2011

[17] DUPLICA INTERNET SOLUTIOS. ¿Qué son los servidores web y por qué son necesarios? [En línea]. Disponible en web: < http://www.duplika.com/blog/que-son-los-servidores-web-y-por-que-son-necesarios > [Consultado 15-03-2013]

[18] MICROSOFT. Proteja su PC [en línea]. Disponible en web: <http://www.microsoft.com/spain/seguridad/content/pc/servidoresfaq.aspx> [Consultado 15-03-2013]

[19] IRON MOUNTAIN. Las cinco mejores prácticas para proteger tus copias de seguridad. 2010. [En línea]. Disponible en web: <http://www.ironmountain.es/~/media/6EB67A91A9D04324830A64AB2B3BD98A.pdf> [Consultado 15-03-2013]

tener en cuenta por que la información manejada en la empresa es de alto nivel de confidencialidad por ende es el activo más importante.

En una entrevista que realizó muycomputerpro en el artículo titulado "Las empresas no pueden sobrevivir sin backup" el señor David Junca importante agente de IT, responsable de Acronis para el sur de Europa, menciona: "Las soluciones de backup y DR son una herramienta esencial. Las empresas no pueden sobrevivir sin ellas. Desde esta perspectiva, la demanda de backup y recuperación de desastres no ha disminuido. Debido a la crisis, algunas empresas están retrasando la adquisición de nuevo software, lo que implica que usan máquinas más viejas con mayor riesgo de caídas y pérdidas de información, lo que aumenta la necesidad de soluciones de backup...".[20]Debido a esto es importante evaluar los diferentes procedimientos que se tienen en cuenta para la realización de backup's en las empresas.

4.2.1. Topología de red manejada en la empresa de contact center

4.2.1.1. Topología en estrella

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información.[21]

Figura 4. Topología de red en estrella. Fuente: Ventas y servicios S.A.

[20] ROJAS Elisabeth. Las empresas no pueden sobrevivir sin backup. 2011. Mcpro muycomputerpro. [En línea]. Disponible en web: <http://www.ironmountain.es/~/media/6EB67A91A9D04324830A64AB2B3BD98A.pdf> [Consultado 19-03-2013]

[21] LAUDON Y LAUDON. Sistemas de Información Gerencial. Nicolás H. Kosciuk. 2006. [En línea]. Disponible en web: < http://ellibrolibre.com.ar/descargas/laudon.pdf >[Consultado 19-03-2013]

Esta topología tiene las siguientes ventajas:

- Solo queda fuera de la red el equipo que se desconecte no afecta a los demás equipos.
- Se pueden agregar nuevos equipos fácilmente.
- Reconfiguración rápida.
- Fácil identificación de daños y/o conflictos.
- Centralización de la red.
- Permite la realización en red de backup's
- Permite la conexión a diferentes servidores remotamente.

4.2.2. Algunas soluciones externas para realización de backup

En el transcurrir del tiempo varias empresas se han enfocado en el desarrollo de sistemas eficientes en la realización de backup's, ya que se ha visto la necesidad de proteger la continuidad de los negocios y contrarrestar las preocupaciones con respecto a la perdida de información, a continuación se mencionan dos herramientas para la realización de backup de información.

Las diversas herramientas de software que se encuentran en el mercado están siendo actualmente utilizadas en el desarrollo de proyectos de ingeniería.

4.2.2.1. Bacula - La solución de backup open source basada en red

Es un conjunto de programas de ordenador, que le permite al administrador del sistema para gestionar copias de seguridad, recuperación y verificación de los datos de la computadora a través de una red de máquinas de diferentes tipos. Bacula también puede ejecutar por completo en un solo ordenador y hacer copias de seguridad de varios tipos de medios, incluyendo cinta y disco.[22]

En términos técnicos, es un programa de copia de seguridad basada en cliente / servidor de red. Bacula es relativamente fácil de usar y eficaz, al tiempo que ofrece muchas características avanzadas de almacenamiento que hacen que sea fácil de encontrar y recuperar archivos perdidos o dañados. Debido a su diseño modular, Bacula es escalable desde pequeños sistemas informáticos individuales a los sistemas que consisten en cientos de ordenadores situados en una red grande.[23]

---

[22] SIBBALD KERN Bacula. What is Bacula? 2013. [En línea]. Disponible en web: <http://www.bacula.org/5.0.x-manuals/en/main/main/What_is_Bacula.html> [Consultado 19-03-2013]
[23] Ibid.

4.2.2.2. Symantec

Backup Exec 2012 es un producto integrado que protege entornos físicos y virtuales, simplifica las copias de seguridad y la recuperación después de un desastre, y ofrece capacidades inigualables de recuperación. Basado en la tecnología V-Ray de Symantec, Backup Exec 2012 restaura servidores enteros, aplicaciones críticas de Microsoft y entornos virtuales VMware o Microsoft Hyper-V para minimizar significativamente el tiempo fuera de servicio de la empresa.[24]

4.2.2.3. Amazon S3 - Backup's online

Ofrece un entorno altamente resistente, escalable y seguro para la copia de seguridad y el archivado de sus datos más importantes. Podrá utilizar la función control de versiones de Amazon S3 para proteger aún mejor sus datos almacenados. Si cuenta con conjuntos de datos de un tamaño significativo, podrá utilizar aws import/export para trasladar grandes cantidades de datos hacia y desde AWS utilizando dispositivos de almacenamiento físicos. Resulta ideal para trasladar grandes cantidades de datos para copias de seguridad de datos periódicas, o para recuperar rápidamente datos en situaciones de recuperación de desastres. También puede definir reglas para archivar conjuntos de objetos de Amazon S3 en el servicio de almacenamiento de coste extremadamente bajo de Amazon Glacier basado en la duración de los objetos. Cuando los datos envejecen, estas reglas le permitirán garantizar que se almacenan automáticamente en la opción de almacenamiento que le resulte más rentable.[25]

4.2.3. Casos éxito en realización de backup's

La realización de una buena práctica de backup's actualmente es un proceso importante para las organizaciones, debido a razones expuestas anteriormente, por ello a continuación se destacan 2 casos éxito en la realización de backup implementados por empresas en diferentes partes del mundo con diferentes herramientas del mercado.

4.2.3.1. Globosat Programadora Ltda.

Productora de 95 de los 100 programas de televisión más populares de Brasil, tiene cierta información valiosa que proteger. La empresa optimizó sus copias de seguridad con Symantec Backup Exec y Backup Exec System Recovery, y eliminó gastos de 114.000 USD en compras de servidores. Además, Globosat confía en Symantec Endpoint Protection para bloquear unidades USB y aplicaciones no autorizadas, lo que elimina las interrupciones debidas a software malicioso y genera ganancias de 50.000 USD por año derivadas de la productividad de usuarios. Dejar de utilizar los dispositivos IDS ahorrará a Globosat un monto estimado de 60.000 USD en gastos de consultoría y licencias.[26]

---

[24] SYMANTEC CORPORATION. Symantec Backup Exec. 2013 [En línea]. Disponible en web: <http://www.symantec.com/es/mx/backup-exec>[Consultado 19-03-2013]

[25] AMAZON WEB SERVICES. Amazon Simple Storage Service (Amazon S3). 2013. [En línea]. Disponible en web: < http://aws.amazon.com/es/s3>[Consultado 25-03-2013]

4.2.3.2. FGC toma un tren rápido hacia el Backup y Recuperación de VMs

El equipo de TI de FGC analizó dos herramientas de backup y eligió Veeam® Backup & Replication™.

"La tasa de rentabilidad era mucho más atractiva con Veeam, " comentó Mondragón. "Veeam representa un gran valor porque posee funcionalidades integradas que lo hacen rápido, eficiente, fiable y fácil de usar."

Veeam está diseñado específicamente para la virtualización y unifica el backup y la replicación en una única solución que proporciona recuperación rápida, flexible y fiable de aplicaciones virtualizadas y datos en VMware vSphere y Microsoft Hyper-V.

Mondragón afirmó que Veeam era más rápido que su herramienta de backup anterior, lo que le permitía realizar backup de VMs con más frecuencia. Además es más, lo cual es un alivio para Mondragón porque antes de que se implementara Veeam, la mayoría de los backup's de sus VMs no se completaban con éxito y debían ejecutarse nuevamente. Los archivos de backup necesitan la mitad del espacio de almacenamiento, gracias a la compresión y des duplicación integrada de Veeam.

"La velocidad del backup es realmente importante, pero el beneficio real para nosotros es una recuperación rápida," comentó Mondragón. "Restaurar una VM solía llevarnos hasta ocho horas, pero ahora lo podemos hacer en una fracción de ese tiempo. Y podemos restaurar archivos guest individuales sin restaurar toda la VM."[27]

---

[26] SYMANTEC CORPORATION. Symantec Backup Exec. 2013 [En línea]. Disponible en web: <https://www.symantec.com/es/mx/resources/customer_success/detail.jsp?cid=globostat_programadora_ltda> [Consultado 25-03-2013]

[27] VEEAM® SOFTWARE. FGC toma un tren rápido hacia el Backup y Recuperación de VMs. 2013 [En línea]. Disponible en web: <http://www.veeam.com/es/success-stories/fgc-toma-un-tren-rapido-hacia-el-backup-y-recuperacion-de-vms.html>>[Consultado 25-03-2013]

5. METODOLOGIA PROPUESTA

Para realizar la metodología se tiene en cuenta el ciclo de vida del proceso, el cual consiste en gestionar procesos desde su creación hasta su finalización, Cada uno de los cinco elementos básicos son:

- Estrategia del proceso: determina los tipos de procesos que deben ser realizados
- Diseño del proceso: identifica los requisitos de proceso y elabora nuevos procesos, así como cambios y mejoras en los ya existentes
- Transición del proceso: genera e implementa procesos nuevos o modificados
- Operación del proceso: lleva a cabo las tareas operativas
- Mejora Continua del proceso: aprende de los éxitos y fracasos del pasado y mejora continuamente la eficacia y eficiencia de los procesos.

5.1. Ciclo de vida del proceso

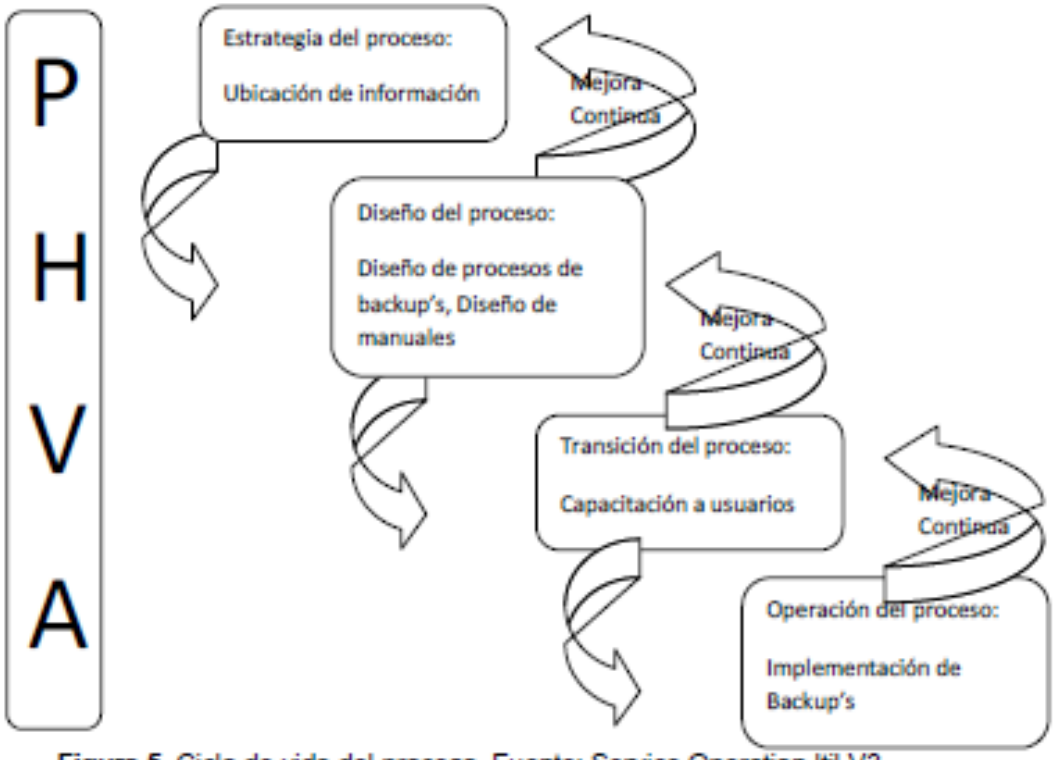


Figura 5. Ciclo de vida del proceso. Fuente: Service Operation Itil V3

4. PROCEDIMIENTO DE RESPALDO Y ADMINISTRACION DE LA INFORMACION.

1. OBJETIVO

Definir los lineamientos que garanticen la ejecución y control de las copias de seguridad de los datos procesados a través de los sistemas de información, los aplicativos desarrollados en la institución y los archivos de los usuarios almacenados en los equipos de cómputo.

2. ALCANCE

Este procedimiento aplica a todos los sistemas y a todos los usuarios que utilizan un PC. La división de Sistemas administra los siguientes backups:

- Sistema operativo
- Software de Servidor
- Bases de datos
- Sitio WEB
- Código Fuente de aplicativos desarrollados en TECNAR

3. DEFINICIONES

3.1 Back up: Copia de seguridad realizada en algún medio de almacenamiento de toda la información que se dispone en un PC de tal forma que se pueda restaurar un sistema después de una pérdida de información.

3.2 Operador: Persona encargada de ejecutar una copia de seguridad.

4. DESCRIPCIÓN DEL PROCEDIMIENTO

De acuerdo a la importancia de la información manejada en la institución, se ha clasificado los backup de la siguiente forma:

- **Back up de Software base:** Permite recuperar la información de los diferentes productos de software instalados tales como: Sistemas operativos (Windows, Linux), Software de aplicación (Word, Excel, Power Point, entre otros). Es responsabilidad de la División de Sistemas.
- **Back up de Código Fuente:** Los aplicativos desarrollados en TECNAR deben ser respaldados teniendo en cuenta el ambiente de desarrollo dada la continuidad con que se crean y modifican los programas. Se debe asegurar la generación de backup de la última versión en producción y de la versión anterior cada vez que se realiza un cambio. Es responsabilidad de la División de Sistemas.
- **Back up de Bases de Datos.** Es responsabilidad de la División de Sistemas y se debe realizar diariamente.
- **Back up de usuarios con PC:** Los usuarios son responsables de la información que resida en el PC asignado y ellos serán los encargados de mantener copia de sus archivos más sensibles.
- **Back up de Servidores.** Es responsabilidad de la División de Sistemas.

Las siglas asignadas para el tipo de backup son:

SB – Software base
BD – Base de datos
CF – Código fuente
PC – Copias de usuarios (Documentos de Word, Excel, pdf, power point, entre otros)

La programación y ejecución de backup es responsabilidad del Jefe de la División de Sistemas, desarrollador de software y los usuarios con PC asignado el cual se debe realizar con una periodicidad diaria, semanal, quincenal o mensual según sea el caso.

La administración de los medios magnéticos de respaldo está a cargo de la División de Sistemas de tal forma que se garantice la confiabilidad y seguridad de estos procesos y de la información proveniente de cada dependencia.

El Jefe de la División de Sistema realiza el primer día hábil de cada mes, la copia del backup de las bases de datos realizada el último día del mes anterior hábil laboralmente. Este DVD es custodiado por el Jefe de la División de Sistemas. El DVD se etiqueta con la nomenclatura DST- AÑO – BD para ser identificado donde DST es la sigla asignada a la dependencia División de sistemas, AÑO indica el año que se le está realizando las copias de seguridad y BD indica el tipo de backup que se está guardando en el medio de almacenamiento

Cada dependencia puede realizar la copia de seguridad de su información en DVD o CD el cual estará bajo la custodia del jefe o director de la dependencia. Cada DVD o CD se etiqueta para ser identificado de acuerdo a la siguiente nomenclatura:

SIGLA DEPENDENCIA – FECHA (dd/mm/aaaa) - # de # - TIPOS DE BACKUP

Las siglas asignadas por dependencia son:

REC – Rectoría
VAC – Vicerrectoría académica
VDI – Vicerrectoría de Desarrollo Institucional
GGR – Gerencia General
GPR – Gerencia de Proyectos y Desarrollo de Nuevos Programas
SGR – Secretaría General
DPL – Dirección de Planeación
FACE – Facultad de Ciencias Económicas
FACI – Facultad de Ciencias de la Ingeniería
FACS – Facultad de Ciencias Sociales
CERES– Facultad de Programa CERES
CCJ – Centro de Conciliación / Consultorio Jurídico
CICTAR– Centro de Investigaciones Científicas y Tecnológicas
CPS – Centro de Proyección Social
CCA – Centro de Calidad Académica
CRNI – Centro de Relaciones Nacionales e Internacionales
CPEC – Centro de Posgrados y Educación Continuada
DST – División de Sistemas
DTH – División de Talento Humano
DFC – División Financiera
DSG – División de Servicios Generales
DRE – División de Recursos Educativos
DBI – División de Bienestar Institucional
DARC – División de Admisiones, Registro y Control Académico
ADM – Admisiones
RCA – Registro y Control Académico
SUM – Suministros
CEA – Centro de Educación a Distancia
CAV – Centro de Ambientes Virtuales

Por ejemplo, La División de Sistemas realiza copia de sus documentos en WORD, EXCEL, PDF en dos DVD y la forma de etiquetarlos sería: **DST - 27/02/2010 – 1 de 2 – PC** y **DST - 27/02/2010 – 2 de 2 – PC**

La vida útil de cada medio magnético es de 06 meses y se debe destruir una vez haya cumplido con su ciclo de vida a excepción de las copias de seguridad de las bases de datos los cuales tiene una vida útil de 3 años.

Toda restauración de backup de las bases de datos debe ser realizada por el Jefe de la División de Sistemas y debe ser notificada a Gerencia por escrito (memorando) indicando los motivos de la restauración.

Se debe permitir la restauración de la información del backup más reciente. Si este falla por alguna circunstancia, se puede recuperar el penúltimo, del antepenúltimo o de cualquier backup hacia atrás según sea el caso.

PROCEDIMIENTO PARA LA ADMINISTRACIÓN DE BACKUP

RESPONSABLE	ACTIVIDADES	DOCUMENTOS Y REGISTROS
Backup de Bases de Datos		
Jefe de la División de Sistemas	Realizar copia de seguridad de las bases de datos de TECNAR. Esta actividad se realiza después de 6:00 P.M de lunes a viernes y los sábados después de 12:30 P.M. excepto días no laborales. Comprimir las copias en un archivo Zip con la nomenclatura: BD_Mes_dia_año.ZIP, y guardarlas en dos diferentes medios de almacenamiento (en el equipo del Jefe de Sistemas y en el Servidor de aplicaciones). Hacer limpieza semana (el último día hábil de cada semana) de los archivos de backup generados, eliminando aquellos que tengan más de un seis días de antigüedad. De igual forma, se realiza la copia de los backup el último día hábil del mes anterior en el DVD donde se almacenas las copias de los backup de las bases de datos del año en mención.	Archivos de backup en los medios de almacenamientos
Backup de Código fuente		
Jefe de la División de Sistemas, Asistente de la División de Sistemas	Realizar copia de seguridad del código fuente cada mes. Esta copia se hace en el equipo del jefe de sistema.	Código fuentes en los medios de almacenamientos
Backup de usuarios con PC		
Usuario del PC	Si el usuario cuenta con las herramientas necesarias para el backup (unidad de CD o DVD, dispositivo USB), elegir la información más sensible de su equipo y sacarle una copia de seguridad en el medio de almacenamiento elegido por él y con la frecuencia que el mismo disponga (diario, semanal, quincenal o mensual). Todos los usuarios, pueden almacenar en una carpeta denominada con su nombre de usuario del PC ubicada en el servidor de dominio de TECNAR (\\192.168.0.3\nombredeusuario) la información que consideran importante y que es necesaria recuperar en caso de daño o deterioro del equipo	Archivos de Backup en medios de almacenamiento y en el servidor de Aplicaciones
Mantenimiento de los DVD de Bases de Datos		
Jefe de la División de Sistemas	Revisar las copias de seguridad en DVD e identificar aquellos DVDs que tengan una vida útil con más de 2 años, los cuales son considerados obsoletos y destruirlos.	
Restauración de Backups de Información de Usuarios		

RESPONSABLE	ACTIVIDADES	DOCUMENTOS Y REGISTROS
Usuario	Identificar la pérdida o daño de información y buscar los respaldos que realizó por protección. En caso de que no localice copias de sus archivos en sus respaldos, solicita al Jefe de Sistema la búsqueda y restauración de la información de los medios ubicados en el servidor de aplicaciones a través de memorando o email.	Memorando o email de solicitud de Restauración de información
Jefe de Sistemas	Recibir la solicitud de restauración de información de la copia ubicada en el servidor de aplicaciones. Verificar la solicitud y aprobar o no la restauración. Si aprueba la restauración, se procede a buscar la información solicitada; en caso de localizarla, realiza una copia de la información y hace entrega por medio de memorando al usuario. En caso de no localizar la información, envía memorando al usuario informando que la información solicitada no se le ha realizado copias de seguridad. **Nota**: La restauración de la información no es aprobada si la solicitud obedece a archivos de un usuario diferente al solicitante.	Memorando.
Restauración de Backups de Información de Bases de Datos		
Usuarios de las Bases de Datos	Identificar la pérdida de información o problemas con las bases de datos e informar a Sistemas por medio escrito las fallas encontradas.	Memorando o Email
Jefe de Sistemas	Realizar verificación de las bases de datos para comprobar la solicitud del usuario. En caso de detectar la perdida de información ya sea por daños en el servidor o borrado involuntario por algún usuario, procede a localizar el backup más reciente para su respectiva restauración. Se informa a los usuarios por email que la base de datos no estará disponible durante el proceso de restauración. Cuando se terminan la restauración, se hacen las pruebas necesarias para comprobar la veracidad y el buen funcionamiento de la misma y se coloca en funcionamiento. Se les informa a los usuarios por email que ya pueden hacer uso de la base de datos.	Solicitud de orden de servicio diligenciada en el Sistema SICOS.
Restauración de Back ups de Código fuente		
Desarrollador de Software, Asistente de Sistemas, Jefe de Sistemas	Detectar la perdida de información de código fuente por daño en el PC o borrado involuntario de líneas de código. Se localiza la copia más reciente del código fuente y se restaura la información.	Código fuente restaurado.

5. CONTROL DE CAMBIOS Y REVISIONES

Revisión	Fecha	Cambio
3	04-09-2009	Se especifica que solo se almacenaran en DVD las copias de Bases de Datos y Código fuente y que dichas copias serán custodiadas por el Jefe de Sistemas y la Gerente General. Se omite el uso de una CDTeca.

		Se adiciona al procedimiento las Siglas GPR: Gerencia de Proyectos y Desarrollo de Nuevos Programas y CERES: Facultad de Programa CERES
4	16-02-2010	Se cambió el tiempo de vida de los DVD de las bases de datos de 6 meses a 2 años. Se especifica la ruta de las carpetas de usuarios para que los usuarios puedan realizar sus copias de seguridad en el servidor de dominio
5	09-03-2011	Se actualiza el logo de la institución dentro del documento.

Elaboró	**Revisó**	**Aprobó**
AGT	CISH	CISH
Fecha: 01-08-2012	**Fecha: 01-08-2012**	**Fecha: 01-08-2012**